

Quandle-like Structures From Groups

Sriram Nagaraj

Department of Electrical Engineering
The University of Texas, at Dallas
Richardson, TX 75083
sriram@student.utdallas.edu

Abstract

We give a general procedure to construct a certain class of "quandle-like" structures from an arbitrary group. These structures, which we refer to as pseudoquandles, possess two of the three defining properties of quandles. We classify all pseudoquandles obtained from an arbitrary finitely generated abelian group. We also define the notion of the kernel of an element of a pseudoquandle and prove some algebraic properties of pseudoquandles via its kernels.

Keywords: knot, link, quandle

Mathematics Subject Classification 2000: Primary 57M27; Secondary 55M99

1 Introduction

Quandles are algebraic structures that have been successfully employed in the study of knots and links since their three defining axioms correspond to the three Reidemeister moves. The presentations of quandles obtained from knot/link diagrams are defined by considering the arcs as generators and the crossings of the arcs as the relations. Quandles were first introduced by Joyce in [1], although the idea of a rack has been available since the 1950's, particularly through the work of Conway and Wraith (see [12] for more details). As a general idea, racks and quandles are the structures obtained from a group G , where the group operation is replaced by conjugation (or n -fold conjugation). This has its own advantages from the group-theoretic point of view since the new structures have (at least in the finite case) nice combinatorial properties. There are a set of (co)homological ideas for theory of racks/quandles as developed in [12] and [8]. We refer the reader to [7],[10],[11] for further discussion of the properties of quandles, which we use later in this paper.

In this introductory section, we recall some basic definitions and examples of racks and quandles, although the canonical reference for the subject is the work by Joyce in [1], [2]. We also introduce the idea of pseudoquandles as algebraic structures satisfying two of the three defining axioms of a quandle and show that we can obtain commutative pseudoquandles from an arbitrary group G (thus, although pseudoquandles do not correspond to all the Reidemeister moves, they are easily obtained from any group). In the following section, we classify all pseudoquandle obtained from an arbitrary finitely generated Abelian group using the fundamental theorem of Abelian groups. We also introduce the idea of the pseudoquandle matrix, an extension of the ideas introduced in [4], and [5] for the case of quandles. In the final section, we define the kernel $\ker(p)$ and cokernel $\operatorname{coker}(p)$ of any element p of a pseudoquandle P and prove some properties of P via the the kernels $\ker(p)$ for each p in P . In essence, the idea of kernels of a pseudoquandle is an abstraction of various concepts introduced in [10], [4], and [5]. Basic results proven there may be generalized using the notion of kernels.

Definition 1.1 A *quandle* is an algebraic structure Q with a closed binary operation $*$: $Q \times Q \longrightarrow Q$ that satisfies the following three axioms:

(i) For all $q \in Q$,

$$q * q = q$$

(ii) Q is a self distributive (from the right) with $*$ as an operation, i.e. for all $p, q, r \in Q$

$$(p * q) * r = (p * r) * (q * r)$$

(iii) For each $p, q \in Q$ there is a unique $r \in Q$ such that $p = r * q$

If Q satisfies axiom (ii) and (iii) above, we call it a **rack**. We also define Q to be a **pseudoquandle** if Q satisfies (i) and (ii). Note that axiom (iii) above is equivalent to the following: For each $q \in Q$, the map $*_q$ from Q into itself defined by:

$$*_q(p) = p * q$$

is bijective. Hence, in view of this, we may define an inverse (or dual) operation $*^{-1}$ of $*$ which satisfies

$$(p * q) *^{-1} q = p$$

for each $p, q \in Q$. We now give some standard examples of quandles. Most of these examples can be found in quandle related literature.

The most basic quandle is the trivial quandle obtained from any set Q with operation

$$a * b = a$$

for all $a, b \in Q$. It can easily be seen that Q a quandle. If $|Q| = n$, it is called the trivial quandle of order n denoted by T_n .

The (classical) example of a quandle is the quandle obtained from an arbitrary group G . By fixing an integer n and defining the operation $*$ on G as:

$$g * h = h^{-n} g h^n$$

we can see that G is a quandle with $*$ as the quandle product. (This is n -fold conjugation in the group G)

There is also a class of quandles called Alexander quandles. An Alexander quandle is a module A over the ring $\mathbb{Z}[t, t^{-1}]$ of formal Laurent polynomials with quandle product $*$ given by:

$$a * b = ta + (1 - t)b \text{ for all } a, b \in A$$

The inverse operation $*^{-1}$ in this case is given by:

$$a *^{-1} b = t^{-1}a + (1 - t^{-1})b \text{ for all } a, b \in A$$

For more details on the classification of finite Alexander quandles, the reader can refer to [7]. In the same vein as Alexander quandles, we can define symplectic quandles as follows:

Let M be a module over a ring R (with characteristic $\neq 2$). Let \langle, \rangle be an anti-symmetric bilinear form $\langle, \rangle : M \times M \rightarrow R$ from $M \times M$ into R . Define the $*$ operation as follows:

$$x * y = x + \langle x, y \rangle y$$

for all $x, y \in M$. It can be shown that M with $*$ as a binary product is a quandle called a symplectic quandle (see [11] for more details).

As a final example, Let $Q = \mathbb{Z}/n\mathbb{Z}$. By defining $*$ on Q as $i * j = 2j - i \pmod{n}$ for all $i, j \in Q$, Q becomes a quandle called a dihedral quandle of order n . Homological methods as applied to these quandles have been developed in [12]

Now, we concentrate on the structures of our study, pseudoquandles obtained from an arbitrary group G . Before we begin, we fix some notation used for the rest of the paper.

Notation: Let G be any group and H a normal subgroup of G . Define G^\triangleleft as follows:

$$G^\triangleleft = \{H \mid H \trianglelefteq G\}$$

We label elements of G^\triangleleft by alphabets $x, y, z \dots$ etc. even though they are actually normal subgroups. Let us define an operation $*$ on G^\triangleleft as follows:

$$x * y = \{ab \mid a \in x, b \in y\}$$

This operation is simply the multiplication of two (normal) subgroups of G . We then have the following:

Proposition 1.2 *The set G^\triangleleft is a commutative monoid with operation $*$ as defined above. Moreover, this operation is self distributive and every element in G^\triangleleft is idempotent with respect to the $*$ operation. Hence, G^\triangleleft is a commutative pseudoquandle with $*$ as the product.*

Proof. Let $x, y \in G^\triangleleft$. Since all of the elements of G^\triangleleft are normal subgroups, their $*$ product is also a normal subgroup, and this operation is commutative by definition of normal subgroups. Since for every (normal) subgroup g of G , $g * g = g$, every element of G^\triangleleft is idempotent. For self distributivity, we have the following string of equalities:

$$\begin{aligned} (y * x) * (z * x) &= y * x * z * x \text{ (by associativity of the } * \text{ product obtained from } G) \\ &= y * z * x * x \text{ (since } x, y, z \text{ are normal)} \\ &= y * z * x = (y * z) * x \end{aligned}$$

for all $x, y, z \in G^\triangleleft$. ■

Whenever we refer to the **pseudoquandle obtained from a group G** , we mean G^\triangleleft with product as given above¹. We shall henceforth denote this structure as P_G . Although P_G constructed from any group G is a pseudoquandle, even for the most basic groups, P_G is not a true quandle. For instance, if $G = \{\pm 1, \pm i, \pm j, \pm k\}$, the quaternion group, every subgroup is normal and hence,

$$P_G = \{\{1\}, \{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}, G\}$$

Consider $p = \{\pm 1, \pm i\}$ and $q = \{\pm 1, \pm j\}$; we see that there is no (normal) subgroup r in P_G such that $p = r * q$.

Since normal subgroups are those objects in the group which are invariant under conjugation, we see that this construction resembles the classical ideology of studying quandles, namely obtaining quandles by conjugation in the group.

2 Pseudoquandles obtained via finitely generated abelian groups

We begin this section with the following observations which motivates the proof of the main result regarding the classification of P_G for any finitely generated abelian group G . In all that follows, let $[n + 1] = \{1, 2, \dots, n + 1\}$ be the first $n + 1$ natural numbers, and p_i is a prime for any positive integer i . Recall that the pseudoquandle obtained from a group G is denoted as P_G .

Proposition 2.1 *The pseudoquandle obtained from $\mathbb{Z}/p^n\mathbb{Z}$, with p a prime number, is isomorphic to $[n + 1]$ with the operation Δ defined as $i \Delta j = \max\{i, j\}$ for all $i, j \in [n + 1]$*

¹Note that G^\triangleleft is self-distributive from both the right and left due to commutativity

Proof. As $\mathbb{Z}/p^n\mathbb{Z}$ is finite and Abelian, the (normal) subgroups of $\mathbb{Z}/p^n\mathbb{Z}$ are the ones generated by elements whose orders are powers of p . We shall denote these (normal) subgroups by x_1, x_2, \dots, x_{n+1} with $x_1 = \{e\}$, $x_{n+1} = \mathbb{Z}/p^n\mathbb{Z}$ so that x_i is a subgroup of x_j iff $i < j$ for all $i, j \in [n+1]$. Also, by definition, $x_i * x_j = \{a + b \mid a \in x_i, b \in x_j\}$, which is precisely $x_{\max\{i,j\}}$. Thus, we need only to verify that $[n+1]$ with Δ is a pseudoquandle. Idempotence is trivial, while self-distributivity follows from the transitivity of $\max\{-, -\}$. ■

Corollary 2.2 *The pseudoquandle obtained from any two finite cyclic groups of the same order are isomorphic.*

Proof. This is immediate from the above proposition. ■

Thus, we see that by creating a pseudoquandle from a finite prime power cyclic group, we cannot "go back" uniquely to the group since we loose information about the prime, so that for instance $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}/q^n\mathbb{Z}$ yield the same pseudoquandle structure for different primes p and q .

Remark: We can renumber the elements of the pseudoquandle as $x_1 = \mathbb{Z}/p^n\mathbb{Z}$, $x_{n+1} = \{e\}$ so that now x_i is a subgroup of x_j iff $i > j$. By this labelling, the pseudoquandle obtained from $\mathbb{Z}/p^n\mathbb{Z}$ is isomorphic to $[n+1]$ with the operation $i \Delta j = \min\{i, j\}$ for all $i, j \in [n+1]$. However, $[n+1]$ with $\min\{-, -\}$ and with $\max\{-, -\}$ as the product are isomorphic as pseudoquandles so there is no confusion.²

We can generalize the above to direct sums to obtain:

Proposition 2.3 *P_G obtained from $G = \mathbb{Z}/p_1^n\mathbb{Z} \oplus \mathbb{Z}/p_2^m\mathbb{Z}$ is isomorphic to $[n+1] \oplus [m+1]$ with binary product given by $(i_1, i_2) * (j_1, j_2) = (\max\{i_1, i_2\}, \max\{j_1, j_2\})$.*

Proof. All the (normal) subgroups of $\mathbb{Z}/p_1^n\mathbb{Z} \oplus \mathbb{Z}/p_2^m\mathbb{Z}$ are of the form (x_i, y_j) with x_i, y_j (normal) subgroups in $\mathbb{Z}/p_1^n\mathbb{Z}, \mathbb{Z}/p_2^m\mathbb{Z}$ respectively with $i, j \in [n+1], [m+1]$ respectively. Thus,

$$(x_{i_1}, y_{j_1}) * (x_{i_2}, y_{j_2}) = (x_{i_1} * x_{i_2}, y_{j_1} * y_{j_2}) = (x_{\max\{i_1, i_2\}}, y_{\max\{j_1, j_2\}})$$

with $i_1, i_2 \in [n+1]$, $j_1, j_2 \in [m+1]$ By the proposition above, the two factors can each be identified with $(\max\{i_1, i_2\}, \max\{j_1, j_2\})$ bijectively. Hence, we can conclude that the pseudoquandle obtained from $\mathbb{Z}/p_1^n\mathbb{Z} \oplus \mathbb{Z}/p_2^m\mathbb{Z}$ is isomorphic to $[n+1] \oplus [m+1]$. ■

Next, we consider the pseudoquandle obtained from $G = \mathbb{Z}$.

Proposition 2.4 *$P_{\mathbb{Z}}$ is isomorphic to \mathbb{Z}_+ (as a pseudoquandle) with product $n * m = \gcd\{n, m\}$.*

Proof. This is trivial since for any two subgroups $n\mathbb{Z}, m\mathbb{Z}$ of \mathbb{Z} , we have that

$$n\mathbb{Z} * m\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z} = \gcd\{n, m\}\mathbb{Z}$$

which can be identified with $\gcd\{n, m\}$ ■

Corollary 2.5 *As pseudoquandles, $P_{\mathbb{Z}} \oplus P_{\mathbb{Z}/p^n\mathbb{Z}}$ is isomorphic to $\mathbb{Z}_+ \oplus [n+1]$*

Proof. This follows readily from the above two propositions. ■

Note that the above corollary holds for a finite direct sum of P_G terms.

We are now ready to state the main result of this section which classifies P_G for any finitely generated abelian group G .

²More generally, if X is an ordered set such that for all x, y in X , $\min\{x, y\}/\max\{x, y\}$ can be defined, one can show that $(X, *)$ with $x * y = \min/\max\{x, y\}$ is a pseudoquandle.

Theorem 2.6 *The pseudoquandle obtained from any finitely generated abelian group G is isomorphic to $L_{n,r} = \mathbb{Z}_+^n \oplus [m_1 + 1] \oplus [m_2 + 1] \dots \oplus [m_r + 1]$ with binary product given by:*

$$(x_1, \dots, x_n, i_1, \dots, i_r) * (y_1, \dots, y_n, j_1, \dots, j_r) = (\gcd\{x_1, y_1\}, \dots, \gcd\{x_n, y_n\}, \max\{i_1, j_1\}, \dots, \max\{i_r, j_r\})$$

For all $x_s, y_s \in \mathbb{Z}$ and $i_t, j_t \in [m_t + 1]$ and positive integers n, m_1, m_2, \dots, m_r

Proof. We shall prove the theorem by using the fundamental theorem of finitely generated abelian groups (primary decomposition form). Any finitely generated abelian group G is isomorphic to

$$\mathbb{Z}^n \oplus \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{m_2}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_r^{m_r}\mathbb{Z}$$

From the above two propositions and corollary, it is clear that the pseudoquandle P_G is isomorphic to $\mathbb{Z}_+^n \oplus [m_1 + 1] \oplus [m_2 + 1] \dots \oplus [m_r + 1]$ with the product as given in the theorem. ■

2.1 The pseudoquandle matrix

In this section, we will give some characterization of the matrix of P_G for arbitrary (finite) groups G . The main definitions are similar to those in the quandle case (see [5], [4]), but we are able to prove more general results in the case of pseudoquandles of the form P_G .

We recall some basic definitions pertaining to the quandle matrix before continuing with our discussion. The quandle/rack/pseudoquandle matrix is simply the multiplication table of the corresponding object written in matrix form:

Definition 2.7 *Let X be a rack (resp. quandle, pseudoquandle) so that $X = \{x_1, x_2, \dots, x_n\}$ for some n . Define the X -matrix M_X as the following:*

$$M_X = \begin{pmatrix} x_1 * x_1 & x_1 * x_2 & \dots & \dots & x_1 * x_n \\ x_2 * x_1 & x_2 * x_2 & & & x_2 * x_n \\ \dots & & \dots & & \dots \\ \dots & & \dots & \dots & \dots \\ x_n * x_1 & x_n * x_2 & \dots & \dots & x_n * x_n \end{pmatrix}$$

As in the case of the quandle matrix, we shall use only the subscript indices to denote the elements of the pseudoquandle matrix to stay consistent with the notation used in literature. Thus M_{P_G} will be an integral matrix, so that the (i, j) element is the subscript of the element $x_i * x_j$. We will always consider the $(1, 1)$ element of the matrix M_{P_G} to be 1, corresponding to the trivial subgroup.

Proposition 2.8 *Let G be any (finite) group. Let P_G be pseudoquandle obtained from G and M_{P_G} be the corresponding integral pseudoquandle matrix. Then, M_{P_G} can be diagonalized.*

Proof. Since P_G is commutative for every group G , we can see that M_{P_G} is a symmetric matrix and hence can be diagonalized by an orthogonal matrix by the spectral theorem. ■

Corollary 2.9 *M_{P_G} is of the form*

$$\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

iff G is simple.

Proof. If G is simple, M_{P_G} is a 2×2 matrix three of whose elements are G and the other the trivial group in the $(1, 1)$ position proving one direction. If M_{P_G} is of the form given in the proposition, then

for each pair of normal subgroup in P_G , x_i, x_j the product of x_i, x_j must some fixed normal subgroup x_k , taking $x_i = \{e\}$, $x_j = G$ we see x_k must be G for each pair (i, j) , which is possible only if G is simple.

$$M_{P_G} = \begin{pmatrix} \{e\} & G \\ G & G \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

■

As in the case of quandle matrices (see [5]), the trace of M_{P_G} is $n(n+1)/2$ with $n = |P_G|$.

In [9] it was noted that analogous ideas may be developed for quandles/racks via permutations of $[n]$ (so that one studies the underlying operation as an element of S_n). This does not yield much fruit in the pseudoquandle case since these do not satisfy the bijection property that quandles/racks do and thus, the map $*_i : [n] \rightarrow [n]$ defined, as usual, by $*_i(j) = j * i$ may not correspond to a permutation of $[n]$ in the case of pseudoquandles.

3 Commutative pseudoquandles and kernels

In this section, we define the main algebraic structure of our study, the kernel $\ker(p)$ of an element p in a commutative pseudoquandle P . We will prove some properties of $\ker(p)$ which motivate our two main results, namely, establishing a bound on the cardinality of certain pseudoquandles via kernels and obtaining a "class equation" for pseudoquandles satisfying an ascending chain criterion (defined later in this section).

Definition 3.1 *Given a pseudoquandle P , the **kernel** of an element $p \in P$ is defined as follows:*

$$\ker(p) = \{q \in P \mid p * q = q * p = p\}$$

*The **cokernel** $\text{coker}(p)$ of $p \in P$, is defined as:*

$$\text{coker}(p) = P - \ker(p) = \{q \in P \mid p * q = q * p \neq p\}$$

In the context of quandle polynomials (see [10]), the cardinality of kernels were used to define the polynomial invariants of quandles but the underlying structure was not analyzed. The results presented there can be generalized via the notion of kernels. We will have more to say in the case of (commutative) pseudoquandles.

In all that follows, let P be a pseudoquandle. A subset R of P is a sub-pseudoquandle if R is a pseudoquandle in its own right. Clearly, any subset closed with respect to the operation in P is a sub-pseudoquandle since self-distributivity and idempotence is obtained from the structure of P .

Proposition 3.2 *$\ker(p)$ is a sub-pseudoquandle for each $p \in P$.*

Proof. If $x, y \in \ker(p)$, then $p * (x * y) = (p * x) * (p * y) = p * p = p$. So that $x * y \in \ker(p)$. Thus, $\ker(p)$ is closed and a sub-pseudoquandle for each $p \in \ker(p)$. ■

Note that $p \in \ker(p)$ for all $p \in P$ and also that $P = \ker(p) \sqcup \text{coker}(p)$ (disjoint union). Also, $\text{coker}(p)$ need not be a sub-pseudoquandle. For example, consider the commutative pseudoquandle $P = \{x_1, x_2, x_3\}$ with the relation $x_i * x_j = x_k$, $i \neq j \neq k$ and $x_i * x_i = x_i$ (this is actually the dihedral quandle on $\mathbb{Z}/3\mathbb{Z}$). Here, $\ker(x_1) = \{x_1\}$. But $\text{coker}(x_1) = \{x_2, x_3\}$ is not a sub-pseudoquandle since $x_2 * x_3 = x_1 \notin \text{coker}(x_1)$. However, there is a sufficient condition to ensure that $\text{coker}(p)$ is a sub-pseudoquandle:

Proposition 3.3 *Let $P = \{p_1, p_2, \dots, p_n\}$. If $\ker(p_1) \subseteq \ker(p_2) \subseteq \dots \subseteq \ker(p_n)$ then, $\text{coker}(p_i)$ is a sub-pseudoquandle for $i = 1, 2, \dots, n$.*

Proof. Since $p_1 \in \ker(p_1) \subseteq \ker(p_2)$, $p_1 \in \ker(p_2)$. Likewise, p_1 and $p_2 \in \ker(p_3)$ etc. so that

$$p_1, p_2, \dots, p_n \in \ker(p_n)$$

But also, $\ker(p_n) \subseteq P$, which shows that $P = \ker(p_n)$. Let us assume that $x, y \in \text{coker}(p_i)$. This implies that $p_i \in \ker(x)$ and $p_i \in \ker(y)$ by the ascending kernel assumption. Thus,

$$p_i * (x * y) = (p_i * x) * (p_i * y) = x * y \neq p_i$$

so that $x * y \in \text{coker}(p_i)$, proving the proposition. ■

Remark: The condition $\ker(p_1) \subseteq \ker(p_2) \subseteq \dots \subseteq \ker(p_n)$ is satisfied, for example, by P_G with $G = \mathbb{Z}/p^{n-1}\mathbb{Z}$ for positive integers n . We will refer to this as the **ascending chain criterion**. Note that this implies that $P = \ker(p_n)$.

Next, we show what happens in the intersection of two kernels. It is interesting to note that the intersection of kernels may not always be a kernel of another element of the pseudoquandle.

Proposition 3.4 For $p, q \in P$, $\ker(p) \cap \ker(q) \subseteq \ker(p * q)$

Proof. If $x \in \ker(p) \cap \ker(q)$, $x * p = p$ and $x * q = q$. Thus, $x * (p * q) = (x * p) * (x * q) = p * q$ so that $x \in \ker(p * q)$. ■

We will now prove a few results analyzing the structure of finite, commutative quandles via kernels. The discussion will motivate the class equation for pseudoquandles satisfying the ascending chain criterion.

Proposition 3.5 For $p, q \in P$ if $p \in \ker(q)$ then $\ker(p) \subseteq \ker(q)$

Proof. Let $x \in \ker(p)$. We need to show that $x * q = q$. Now, $p * q = q$, and $x * p = p$. We also have the following:

$$x * q = x * (p * q) = (x * p) * (x * q) = p * (x * q)$$

But,

$$p * (x * q) = (p * x) * (p * q) = p * q = q$$

so that $x * q = q$. ■

Analogous to any other algebraic structure, we can defined the product of two subsets of a quandle/rack/pseudoquandle etc. with respect to the operation binary operation inherited from the parent structure.

Definition 3.6 For any subsets A, B of P , define

$$A * B = \{a * b \mid a \in A, b \in B\}$$

and

$$A^2 = A * A$$

We have that the $\ker(p)$ is idempotent as a set with the above definitions:

Proposition 3.7 For all $p \in P$, $[\ker(p)]^2 = \ker(p)$

Proof. Let $\ker(p) = \{p_1, p_2, \dots, p_k\}$. Thus, $\ker(p) * \ker(p) = \{p_i * p_j \mid i, j = 1, 2, \dots, k\}$. Since $p_i * p_i = p_i$, $\ker(p) \subseteq [\ker(p)]^2$. Also $\ker(p)$ is a sub-pseudoquandle, so that $p_i * p_j \in \ker(p)$ for all $p_i, p_j \in \ker(p)$, showing that $[\ker(p)]^2 \subseteq \ker(p)$. Thus, $[\ker(p)]^2 = \ker(p)$. ■

If $\{p\}$ denotes the single element sub-pseudoquandle, it is easy to see that $\{p\} * \ker(p) = \{p\}$. Infact, more is true:

Proposition 3.8 For any $p, q \in P$, $\{q\} * \ker(p)$ is a sub-pseudoquandle

Proof. Let $x, y \in \{q\} * \ker(p)$. Thus, $x = q * p_1$ and $y = q * p_2$ where p_1 and $p_2 \in \ker(p)$. Clearly, $x * y = q * (p_1 * p_2)$ which is an element of $\{q\} * \ker(p)$. Like before, idempotence and self-distributivity follow from multiplication in P . ■

The next lemma will be required for establishing a lower bound on the cardinality of a pseudoquandle whose kernels and cokernels satisfy certain intersection criteria.

Lemma 3.9 If $p, q \in P$, and $\ker(p) \cap \ker(q) = \phi$, then $\ker(q) \subseteq \text{coker}(p)$ and $\ker(p) \subseteq \text{coker}(q)$

Proof. Since $P = \ker(p) \sqcup \text{coker}(p)$,

$$P \cap \ker(q) = (\ker(p) \sqcup \text{coker}(p)) \cap \ker(q) = (\ker(p) \cap \ker(q)) \sqcup (\text{coker}(p) \cap \ker(q))$$

but $\ker(p) \cap \ker(q) = \phi$ by our assumption. Thus $\ker(q) = \text{coker}(p) \cap \ker(q)$ showing that

$$\ker(q) \subseteq \text{coker}(p)$$

The other inclusion is entirely similar. ■

A simple application of the above proposition gives us the lower bound on the cardinality of P , when $|\ker(p)| = |\ker(q)| = k$.

Corollary 3.10 If $p, q \in P$, and $\ker(p) \cap \ker(q) = \phi$ with $|\ker(p)| = |\ker(q)| = k$, then $|P| \geq 2k$

Proof. $P = \ker(p) \sqcup \text{coker}(p)$. So $|P| = |\ker(p)| + |\text{coker}(p)|$. But by the above corollary, $\text{coker}(p)$ contains $\ker(q)$, so that $|\text{coker}(p)| \geq |\ker(q)|$. Hence, $|P| \geq |\ker(p)| + |\ker(q)| = 2k$. ■

Let us define

$$P^{\ker} = \{\ker(p) \mid p \in P\}$$

We will now show that the map $\varphi : P \rightarrow P^{\ker}$ defined by $\varphi(p) = \ker(p)$ is bijective.

Proposition 3.11 The map φ defined above is bijective

Proof. We will first show that $p = q \iff \ker(p) = \ker(q)$. If $p = q$, it is clear that $\ker(p) = \ker(q)$. For the other direction, $\ker(p) = \ker(q)$ implies that $q \in \ker(p)$ and $p \in \ker(q)$, so $p = q * p = p * q = q$. Hence, φ is injective. Also, φ is clearly surjective hence is a bijection. ■

We now come to the other main result of this section. Before this, we will define a few terms used in the result.

Definition 3.12 Let $p \in P$ and $q \in \ker(p)$. The **relative cokernel** of q in p is $\ker(p) - \ker(q)$ written as $\text{coker}(q : p)$. If $q \notin \ker(p)$, we define $\text{coker}(q : p) = \phi$. Thus

$$\text{coker}(q : p) = \{s \in \ker(p) \mid s * q \neq q\} = \ker(p) - \ker(q)$$

The cardinality of $\text{coker}(q : p)$ is defined to be the **index** of q in p .

The following theorem is a pseudoquandle version of Lagrange's theorem in group theory.

Theorem 3.13 Let $p \in P$ and $q \in \ker(p)$. Then, $|P| = |\ker(q)| + |\text{coker}(p)| + |\text{coker}(q : p)|$.

Proof. $P = \ker(p) \sqcup \text{coker}(p)$ so that

$$\begin{aligned} P - \ker(q) &= (\text{coker}(p) \sqcup \ker(p)) - \ker(q) \\ \implies \text{coker}(q) &= \text{coker}(p) \sqcup (\ker(p) - \ker(q)) \\ \implies \text{coker}(q) &= \text{coker}(p) \sqcup \text{coker}(q : p) \end{aligned}$$

But also, $P = \ker(q) \sqcup \text{coker}(q) = \ker(q) \sqcup (\text{coker}(p) \sqcup \text{coker}(q : p))$. Taking cardinalities,

$$|P| = |\ker(q)| + |\text{coker}(p)| + |\text{coker}(q : p)|$$

■

The following is an application of the above ideas and is a "class equation" of pseudoquandles satisfying the ascending chain criterion. It is similar to the class equation for finite groups in terms of (the cardinalities of) conjugacy classes.

Theorem 3.14 *Let $P = \{p_1, p_2, \dots, p_n\}$ with $\ker(p_1) \subseteq \ker(p_2) \subseteq \dots \subseteq \ker(p_n)$. Then*

$$|P| = |\ker(p_1)| + \sum_{k=1}^{n-1} |\text{coker}(p_k : p_{k+1})|$$

Proof. It was remarked above that $\ker(p_1) \subseteq \ker(p_2) \subseteq \dots \subseteq \ker(p_n)$ implies $P = \ker(p_n)$. Now, we have the following manipulation:

$$\ker(p_n) = (\ker(p_n) - \ker(p_{n-1})) \sqcup \dots \sqcup (\ker(p_2) - \ker(p_1)) \sqcup (\ker(p_1))$$

Taking cardinalities on both sides, we see that $|P| = |\ker(p_n)| = |\ker(p_1)| + \sum_{k=1}^{n-1} |\text{coker}(p_k : p_{k+1})|$. ■

We close the section with the following observation regarding the behaviour of kernels of a pseudoquandle under a homomorphism:

Proposition 3.15 *Let $\theta : P \rightarrow Q$ be a homomorphism of pseudoquandles. Then, $\theta(\ker(p)) \subseteq \ker(\theta(p))$ for each $p \in P$. There is equality of sets if θ is an isomorphism.*

Proof. Let $x \in \ker(p)$. Then $\theta(x) * \theta(p) = \theta(x * p) = \theta(p)$. Hence, $\theta(x) \in \ker(\theta(p))$. If θ is an isomorphism, and $\theta(x) \in \ker(\theta(p))$ then clearly $\theta(x) * \theta(p) = \theta(p) = \theta(x * p)$ which implies $x * p = p$, thus they two sets are equivalent. ■

The restriction of an isomorphism between two pseudoquandles to kernels results in an induced isomorphism. If P and Q are isomorphic, say via Φ , the restriction of Φ to each $\ker(p_i)$ induces an isomorphism $\Phi|_{\ker(p_i)}$ between the kernels $\ker(p_i)$ and $\ker(q_i)$ for each $i = 1, 2, \dots, n$. Clearly, for $p \in \ker(p_i) \cap \ker(p_j)$, $\varphi_i(p) = \varphi_j(p)$.

The converse to the above may not always be true. However, it is easily seen to be true in the case of pseudoquandles satisfying the ascending chain criterion. In that case, we can characterize (upto isomorphism) a pseudoquandle from its constituent kernels.

References

- [1] D. Joyce, A Classifying Invariant of Knots, The Knot Quandle, *J. Pure Appl. Algebra* **23** (1982), pp. 37–65.
- [2] D. Joyce, Simple quandles, *J. Algebra* **792** (1982), pp. 307–318.

- [3] M. Grana, N. Andruskiewitsch, From Racks to pointed Hopf Algebras, *Adv. in Math.* **178** (2003), pp. 177-243
- [4] S. Nelson, J Vo, Matrices and Finite Biquandles, *Homology, Homotopy and Applications* **8** (2006) pp. 51-73
- [5] S Nelson, B Ho, Matrices and Finite Quandles, *Homology, Homotopy and Applications*, **7** (2005), pp.197-208
- [6] I. M Isaacs, Algebra: A Graduate Course, Brooks Cole 1 edition (November 15, 1993)
- [7] S. Nelson, Classification of finite Alexander Quandles, *Topology Proceedings* **27** (2003) pp. 245-258
- [8] J. S. Carter, D. Jelsovsky, S. Kamada, M. Saito, Quandle Homology Groups, Their Betti Numbers, and Virtual Knots Arxiv.org, <http://arxiv.org/abs/math/9909161>
- [9] P Lopes, D Roseman, On Finite Racks and Quandle, Arxiv.org: http://arxiv.org/PS_cache/math/pdf/0412/0412487v1.pdf
- [10] S Nelson, A Polynomial Invariant of Finite Quandles, Arxiv.org: http://arxiv.org/PS_cache/math/pdf/0702/0702038v3.pdf
- [11] E A Navas, S Nelson, On Symplectic Quandles, Arxiv.org: <http://arxiv.org/abs/math/0703727>
- [12] J Przytycki, M Niebrzydowski, Homology of Dihedral Quandles, Arxiv.org: <http://arxiv.org/abs/math/0611803>